Amendments to the Claims

1. - 2. (canceled)

3. (currently amended) A system as recited in claim 30 [[1]], further comprising:

a storage unit coupled to the encryption accelerator arranged to store at least a portion of the data to be encrypted.

4-9. (canceled)

10. (currently amended) A system as recited in claim 30 [[9]], wherein the encryption accelerator is selectively operable in an Initial Mode and a Continuation mode wherein the Initial Mode the system operates in a sequential manner whereas in the continuation mode the state memory is reloaded with ~~the~~ stored state memory values.

11. (currently amended) An encryption accelerator arranged to encrypt and decrypt data formed of a plurality of bytes using an RC4 stream cipher, comprising:

a combinational logic block arranged to perform a pre-determined logic operation on selected input values;

a state memory array coupled to the combinational logic block ~~arranged to store a plurality of state memory values~~ having a plurality of memory locations; and

a state machine coupled to the combinational logic block and the state memory ~~array~~, the state machine configured to: [,]

initialize via hardware an incrementing pattern of substitution values in the state memory ~~array~~, each substitution value stored in a separate memory location,

perform a first RC4 shuffling operation using a portion of ~~the~~ a key array received from a system memory, wherein the first RC4 shuffling operation is performed concurrently with the receipt of [[a]] the portion of the key array,

generate a ~~pseudo-random number~~ random byte as a result of a second RC4 shuffling operation;

byte-wise transfer a portion of the data to the combinational logic block as a first input value,

transfer the generated ~~pseudo-random number~~ random byte to the combinational logic as a second input value,

logically operate on the first and second input values by the combinational logic to form a resulting data byte, and outputting the resulting data byte.

12. (cancel)

13. (current amended) An accelerator as recited in claim 11 [[12]], wherein the accelerator is coupled to the [[a]] system memory arranged to store the ~~secret~~ key array and wherein the accelerator is coupled to a CPU in such a way that the accelerator operates to encrypt the data so as to preserve CPU resources.

14. (original) An accelerator as recited in claim 13, where the CPU is coupled to the accelerator and the system memory by way of a system bus.

15. (original) An accelerator as recited in claim 11, further comprising an input latch coupled to the state machine, the state memory array, and the combinational logic block arranged to store the data to be encrypted.

16. (original) An accelerator as recited in claim 11, further comprising an output latch coupled to the state machine, the state memory array, and the combinational logic block arranged to store the encrypted data.

17. (original) An accelerator as recited in claim 11, wherein the logic function is an exclusive OR logic function.

18. (original) An accelerator as recited in claim 14, wherein the data to be encrypted is passed to the input latch by way of the system bus as directed by the CPU.

19. (original) An accelerator as recited in claim 18, wherein the encrypted data is passed to external circuitry as directed by the CPU by way of an output node coupled to the system bus.

20. (original) An accelerator as recited in claim 11, wherein the accelerator further includes a first index counter and a second index counter each of which is connected to and directed by the state machine.

21. (original) An accelerator as recited in claim 11, wherein the accelerator is included in a computing device.

22. (previously presented) An accelerator as recited in claim 21, wherein the computing device is connected to one of the computing devices of the network, wherein the accelerator encrypts a sent message sent to at least one of the network of computing devices and wherein the accelerator decrypts a received message from at least one of the network computing devices.

23. (currently amended) The system of claim 30 [[1]], wherein the ~~hardware-based encryption accelerator~~ state machine is further configured to direct ~~generate a pseudorandom number as a result of~~ a second RC4 shuffling to generate a random byte.

24. (currently amended) The system of claim 23, wherein the hardware-based encryption accelerator includes a combinational logic block configured to exclusive OR the generated ~~pseudorandom~~ random byte ~~number~~ with a byte of the data.

25. (currently amended) A method for performing an RC4 stream cipher in a hardware-based ~~encryption~~ cryptographic accelerator, comprising:

(a) initializing a state memory having a plurality of memory locations with an incrementing pattern of substitution values;

(b) receiving, at the hardware-based encryption accelerator, a portion of a key array;

(c) upon direction of a state machine, shuffling the pattern of substitution values in the state memory [[,]] using an RC4 shuffling operation, wherein the shuffling is performed concurrently with the receipt of the portion of the key array , and wherein the shuffling operation is completely performed within the cryptographic accelerator; and

(d) repeating steps (b) and (c) until each portion of the key array has been received.

26. (currently amended) The method of claim 25, further comprising:

(e) generating a ~~pseudo-random~~ random number using a second RC4 shuffling operation.

27. (currently amended) The method of claim 26, further comprising:

(f) exclusively ORing the ~~pseudo-random~~ random number with a portion of an input data.

28. (previously presented) The method of claim 27, wherein the input data is plaintext.

29. (previously presented) The method of claim 27, wherein the input data is ciphertext.

30. (new) A system for performing cryptographic operations using an RC4 stream cipher, comprising:

a cryptographic accelerator including:

a state memory having a plurality of memory locations, wherein the state memory is configured to store a plurality of substitution values associated with the RC4 stream cipher, each substitution value stored in a separate memory location, and

a state machine coupled to the state memory, wherein the state machine is configured to direct an RC4 shuffling operation by which the plurality of substitution values are moved to different memory locations within the state memory,

wherein the shuffling operation is completely performed within the cryptographic accelerator; and

a processor coupled to the cryptographic accelerator.

31. (new) The system of claim 30, wherein the state machine directs portions of a key array to be retrieved from a system memory and wherein the shuffling operation is performed upon receipt of each portion of the key array.